A Brief Understanding Of the PoPI Act

The purpose of the PoPI Act is to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and sharing another entity's personal information by holding them accountable should they abuse or compromise your personal information in any way. The PoPI legislation basically considers your personal information to be "precious goods" and therefore aims to bestow upon you, as the owner of your personal information, certain rights of protection and the ability to exercise control over:

when and how you choose to share your information (requires your consent)

the type and extent of information you choose to share (must be collected for valid reasons)

transparency and accountability on how your data will be used (limited to the purpose) and notification if/when the data is compromised

providing you with access to your own information as well as the right to have your data removed and/or destroyed should you so wish

who has access to your information, i.e. there must be adequate measures and controls in place to track access and prevent unauthorised people, even within the same company, from accessing your information

how and where your information is stored (there must be adequate measures and controls in place to safeguard your information to protect it from theft, or being compromised)

the integrity and continued accuracy of your information (i.e. your information must be captured correctly and once collected, the institution is responsible to maintain it)

Examples of "personal information" for an individual could include:

Identity and/or passport number

Date of birth and age

Phone number/s (including mobile phone number)

Email address/es

Online/Instant messaging identifiers

Physical address

Gender, Race and Ethnic origin

Photos, voice recordings, video footage (also CCTV), biometric data

Marital/Relationship status and Family relations

Criminal record

Private correspondence

Religious or philosophical beliefs including personal and political opinions

Employment history and salary information

Financial information

Education information

Physical and mental health information including medical history, blood type, details on your sex life

Membership to organisations/unions

It must however be noted that some personal information, on its own, does not necessarily allow a third party to confirm or infer someone's identity to the extent that this information can be used/abused for other purposes. The combination of someone's name and phone number and/or email address for example is a lot more significant than just a name or phone number on its own. As such the Act defines a "unique identifier" to be data that "uniquely identifies that data subject in relation to that responsible party".

We have to accept that we now live in an information age and along with this progress comes the responsibility for each person to take care of and protect their own information. Do not accuse someone else of sharing or compromising your personal information when you publish the very same information on public services like Facebook, LinkedIn, Google+ or public directories. Modern technology makes it easy to access, collect and process high volumes of data at high speeds. This information can then be sold, used for further processing and/or applied towards other ends. In the wrong hands such an ability can cause irreparable harm to individuals and companies. To protect your right to privacy and abuse of your information, data protection legislation is necessary even if it means imposing some social limits on society to balance the technological progress. So remember: The PoPI Act cannot protect you if you do not take care to protect yourself.

It is important to note though that this right to protection of "personal information" is not just applicable to a natural person (i.e. an individual) but any legal entity, including companies and also communities or other legally recognised organisations. All of these entities are considered to be "data subjects" and afforded the same right to protection of their information. So this means that while you as a consumer now have more rights and protection, you and your company/organisation are considered "responsible parties" and have the same obligation to protect other parties personal information. As a company this would include protecting information about your employees, suppliers, vendors, service providers, business partners, etc.

The PoPI legislation is not a rare or unique phenomenon to South African law. Many countries have similar legislation in place to protect the personal information of their "data subjects", including rules and regulations for international (cross-border) transfer and sharing of data. The general consensus seems to be that, apart from an unrealistic implementation period of one year and some practical implementation challenges, the PoPI Act is well thought out and it borrows from the "best of" other similar international laws, learning from their mistakes and shortcomings.

As usual, ignorance of the law is no excuse. Incorporating PoPI into the day-to-day operations of a business will most likely require a significant amount of time and effort, including: educating and training staff, updating business processes and implementing or updating technology solutions. Early action is essential, especially if you do not have a business nervous system (BNS) to facilitate this. Consider for example that under the PoPI Act you could be breaking the law if you do something as

simple as synchronising your contacts on your phone, sending an email with sensitive content, taking/sharing a video or photo, using an international mail provider (like Google…) and so forth